IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NORTH DAKOTA

SpoofCard, LLC and Amanda Pietrocola, Plaintiffs, v. The Hon. Wayne Stenehjem, Attorney General of the State of North Dakota, in his Official Capacity, Defendant.	**STATE OF NORTH DAKOTA'S RESPONSE TO SPOOFCARD'S MOTION FOR PARTIAL SUMMARY JUDGMENT** **Case No. 1:19-cv-00276**

INTRODUCTION

SpoofCard filed a motion for partial summary judgment arguing in its brief that North Dakota's Anti-Spoofing Act is preempted by federal law. See Dist. Ct. Doc. ID #18. But unlike the law challenged in Mississippi that targeted both misleading ***and*** fraudulent spoofing, North Dakota's law targets fraudulent spoofing only, not the limited legitimate spoofing permitted by federal law. Thus, North Dakota's law is not preempted because it does not stand as an obstacle to the accomplishment of the objectives of federal law.

SpoofCard also argues the Act violates the Commerce Clause. See id. But SpoofCard acknowledges North Dakota's law does not regulate callers who reasonably believe the recipient of their call is not physically within North Dakota. Even if burdensome, it is clearly possible for SpoofCard and its customers to make a reasonable determination that some call recipients are located within North Dakota. Those calls are the only ones regulated by the Anti-Spoofing Act. In other words, the Act's regulatory reach simply does not extend outside of North Dakota. As a consequence, North Dakota's law does not have the practical effect of regulating commerce occurring wholly outside the State's borders, and does not violate the Commerce Clause.

The State files this brief in response to SpoofCard's motion for partial summary judgment. The State requests the Court to deny SpoofCard's motion and grant the State's cross-motion for summary judgment.

LAW AND ARGUMENT

I. The Anti-Spoofing Act's regulation of fraudulent spoofing does not conflict with federal law and is therefore not preempted.

SpoofCard's primary contention is that North Dakota's Anti-Spoofing Act conflicts[1] with federal law because of a distinction between merely deceptive spoofing, and the fraudulent spoofing that causes harm. That distinction is irrelevant to a conflict preemption analysis of North Dakota's law. North Dakota's law, like federal law, targets the fraudulent spoofing that causes harm. North Dakota's law does not target the limited non-harmful but deceptive spoofing permitted by federal law. Compare N.D. Cent. Code § 51-28-08.1(1)(a) (indicating a person may not "[t]ransmit misleading or inaccurate caller identification information with the *intent to defraud or cause harm*") (emphasis added) with 47 U.S.C. § 227(e)(1) (indicating a person may not "knowingly transmit misleading or inaccurate caller identification information with the *intent to defraud, cause harm, or wrongfully obtain anything of value*") (emphasis added). Because North Dakota's law and federal law both target fraudulent harmful spoofing, their purposes and objectives are the same and do not conflict.

SpoofCard's reliance upon the Fifth Circuit's decision in TelTech Systems, Inc. v. Bryant, 702 F.3d 232 (5th Cir. 2012), is misplaced. The Mississippi law at issue in Bryant was held preempted precisely because it targeted not only fraudulent spoofing, but also the deceptive or misleading spoofing permitted by federal law. See Bryant, 702 F.3d at 234 ("ASA [Mississippi's Act] is more restrictive than TCIA. On the one hand, spoofing done with 'intent to defraud, cause harm, or wrongfully obtain anything of value (harmful spoofing), in violation of TCIA, is also violative of ASA. On the other hand, spoofing done without such intent, but 'with the intent to deceive . . . or mislead the recipient of the call'

[1] The parties agree the preemption issue here is limited to whether the Anti-Spoofing Act conflicts with the Truth in Caller ID Act (TCIA). SpoofCard has not advanced any arguments that the TCIA expressly preempts state regulation, or that Congress has impliedly preempted the entire field of state regulation. See Dist. Ct. Doc. ID #18 at 7-14.

(non-harmful spoofing), violates only ASA."); id. at 239 ("[T]here is an inherent federal objective in TCIA to protect non-harmful spoofing. ASA's proscription of non-harmful spoofing – spoofing done without 'intent to defraud, cause harm, or wrongfully obtain anything of value' – frustrates this federal objective and is, therefore, conflict-preempted.").

SpoofCard further argues that North Dakota's law prohibits the deceptive spoofing permitted by federal law because North Dakota's definition of "defraud" includes taking a call recipient's "time." See Dist. Ct. Doc. ID #18, at 12-13 (citing N.D. Cent. Code § 51-28-08.1(5)(c)). But nothing that SpoofCard has cited in the legislative history of the TCIA indicates Congress considered whether or not "time" could be considered something of value. In this respect, the federal law merely set a floor for regulation, not a ceiling. Conflict preemption principles do not restrict North Dakota from enacting more expansive regulation that provides additional definition to what is considered something of value. See, e.g., Wuebker v. Wilbur-Ellis Co., 418 F.3d 883, 888 (8th Cir. 2005) (concluding "the presumption against preemption" applied and precluded preemption where "nothing in the language of the regulation or in its history . . . indicates whether the EPA meant [the federal regulation at issue] to be a regulatory floor or ceiling"); see also Stamps v. Collagen Corp., 984 F.2d 1416, 1424 (5th Cir. 1993) (indicating that when federal law "forms only the floor of regulation, the states are free to construct a regulatory ceiling"). In other words, North Dakota's decision to include "time" as something of value is permissible so long as it does not directly conflict with the federal objective of protecting the limited misleading spoofing permitted by the TCIA.

To the extent the word "time" may conflict directly with the TCIA, the Court must limit any declaratory or injunctive relief granted to SpoofCard to the precise harm caused by the conflict. See, e.g., Califano v. Yamasaki, 442 U.S. 682, 702 (1979) ("[I]njunctive relief should be no more burdensome to the defendant than necessary to provide complete relief to the plaintiffs."); Gerlich v. Leath, 861 F.3d 697, 710 (8th Cir. 2017) ("An

injunction must not be 'broader than necessary to remedy the underlying wrong.'"). Any direct conflict between North Dakota's regulation of "time" and the TCIA's protection of legitimate spoofing can be remedied by severing the single word "time" from the Anti-Spoofing Act. No other provisions of the Act conflict with federal law.

"The severability of the valid portions of a state statute which is otherwise found constitutionally infirm is a matter of state law." ANR Pipeline Co. v. Iowa State Commerce Comm'n, 828 F.2d 465, 473 (8th Cir. 1987) (citing Exxon Corp. v. Eagerton, 462 U.S. 176, 196-97 (1983)). Under North Dakota law, the "declaration of part of a law as unconstitutional does not require the court to declare the entire law invalid unless all provisions are so connected and dependent upon each other that one can conclude that the Legislature intended the law to take effect in its entirety or not at all." State v. Fischer, 349 N.W.2d 16, 18 (N.D. 1984) (citing Arneson v. Olson, 270 N.W.2d 125, 137 (N.D.1978)); see also N.D. Cent. Code § 1-02-20 (stating the Legislature's preference for severability by confining a court's determination of a statute's invalidity "to the clause, sentence, paragraph, section, or part thereof directly involved in the controversy").

The clear focus of North Dakota's Anti-Spoofing Act is to prohibit spoofing done with a fraudulent intent that causes harm. The Legislative Assembly defined the term "defraud" to mean "taking anything of value." N.D. Cent. Code 51-28-08.1(5)(c). The Legislature then included three specific examples of items it deemed valuable, only one of which was "time." See id. (stating things of value include "money, property, or time"). This provision shows the Legislative Assembly clearly intended the regulation of fraudulent spoofing beyond merely taking a call recipient's time. The spoofing targeted by the Legislative Assembly was also meant to prevent the types of harm outlined in the Affidavit of Tonya Hetzler, which can take many serious and harmful forms. See Dist. Ct. Doc. ID #21-1 at ¶¶ 17-18 (describing spoofing that results in identity theft and scams where victims lose large amounts of money).

If the word "time" conflicts with federal law, the remaining portions of the Act will

still be workable by striking that single word from the Act. Regulating the taking of "property" is not connected or dependent upon regulating the taking of "time" such that the Court is prevented from applying the doctrine of severability. The same is true for the regulation of the taking of "money." That regulation can stand independent of the regulation of time. Thus, striking the word "time" and leaving all other portions of the Act intact will still leave a result contemplated and desired by the Legislative Assembly. See North Dakota Legislative Assembly v. Burgum, 916 NW.2d 83, 106 (N.D. 2018) (noting that the valid portions of a legislative act will stand even if a part is unconstitutional "unless the result be one not contemplated or desired by the Legislature") (quoting State ex rel. Link v. Olson, 286 N.W.2d 262, 274 (N.D. 1979). Indeed, it would be perverse if the entire Act was stricken when its most impactful parts (regulating the fraudulent taking of money and property) are entirely consistent with federal law, on the grounds that its least impactful part (regulating the taking of time) conflicts with federal law. Such a result clearly would not have been contemplated or desired by the Legislature.

SpoofCard also contends that North Dakota's Anti-Spoofing Act conflicts with the TCIA in one other aspect. SpoofCard claims that North Dakota cannot prohibit a spoofer from displaying a telephone number she does not own or has not received consent to use from the owner. See Dist. Ct. Doc. ID #18, at 13 (citing N.D. Cent. Code § 51-28-08.1(1)(b)). In fact, SpoofCard boldly asserts that federal protection of legitimate spoofing must give a spoofer the "right to use the number she chooses to spoof . . . even when the caller had no specific legal right to use the spoofed number." Id.

Regulation of property theft plainly falls within the State's historic police powers. E.g., Nebraska Beef Producers Comm. v. Nebraska Brand Comm., 287 F. Supp. 3d 740, 752 (D. Neb. 2018). Nothing that SpoofCard has cited in the legislative history of the TCIA indicates Congress intended to give a spoofer the right to use any number she chooses -- even one she does not own or have consent to use -- in order to mislead or deceive a call recipient. To the contrary, ***none*** of the examples of legitimate spoofing

discussed by the Federal Communications Commission (FCC) in its order implementing the TCIA recognize a spoofer's right to use someone else's phone number without consent. See In the Matter of Rules and Regulations Implementing the Truth in Caller ID Act of 2009, 26 FCC Rcd. 9114, 9117-9118 (2011). Examples of beneficial/non-harmful manipulation of caller ID included: (1) the need for domestic violence shelters to complete a call without revealing the actual number of the shelter; (2) a doctor responding to after-hours messages from a cell phone but who wants to transmit his office number as the calling number rather than a personal cell number; (3) telemarketers substituting the name and customer service number of the seller on whose behalf they are placing a call; or (4) a telecommunication carriers manipulating caller ID to test equipment to emulate customer experience or to investigate fraudulent use of a telecommunications network. Id.

Non-harmful spoofing does not *require* a spoofer to use a telephone number actually owned by another person in order to deceive a call recipient. Furthermore, neither of the TCIA's two express exceptions grant an across-the-board right for any spoofer to use or display a telephone number he does not own, or has not received consent to use from the owner, as a means of engaging in deceptive spoofing. See 47 U.S.C. § 227(e)(3)(B)(ii) (exempting "any authorized activity of a law enforcement agency; or . . . a court order that specifically authorizes the use of caller identification manipulation"); see also 47 C.F.R. § 64.1604(b)(1) & (2) (exempting "authorized …activity of law enforcement agency of the United States, a State, or a political subdivision of a State"; or "pursuant to a court order that specifically authorizes the use of caller identification manipulation."). The FCC expressly "decline[d] to adopt any other exemptions from the Act" that commenters asserted were other non-harmful forms of spoofing. In the Matter of Rules Implementing the TCIA of 2009, 26 FCC Rcd. at 9123-24.

If the Court accepts SpoofCard's assertion that the TCIA gives spoofers the

unlimited right to use any phone number they choose to carry out a deception, it would have to recognize that federal law protects the ability to falsely impersonate the Director of the North Dakota Department of Health, the State Bank of North Dakota, the Social Security Administration, the Internal Revenue Service, Medicare, legitimate businesses, and many others. The display of someone else's actual phone number without consent is itself harmful. See Hetzler Aff., Dist. Ct. Doc. ID #21-1 at ¶¶ 12-19. Not only is it the gateway to many different types of fraudulent schemes, but it hinders law enforcement's ability to investigate the fraud. Id. at ¶¶ 9, 11-12. A spoofer's use of a business's actual number without consent causes harm to the business's reputation even if a spoofer is not successful in carrying out a scam, because angry people believe the spoofed call was generated by the business itself. Id. at ¶ 23. It would be absurd to construe the TCIA's limited protection of legitimate spoofing as permitting this form of property theft/misuse when the spoofing protected by the TCIA can be done by using a telephone number the spoofer owns or has the consent to use (or simply unassigned numbers no one owns).

II. The Anti-Spoofing Act does not violate the Commerce Clause.

As anticipated, SpoofCard's primary Commerce Clause challenge is brought under the extraterritoriality doctrine of Healy v. Beer Institute, Inc., 491 U.S. 324 (1989). SpoofCard contends that North Dakota's law effectively regulates commerce occurring entirely outside of North Dakota. See Healy, 491 U.S. at 336 ("The critical inquiry is whether the practical effect of the regulation is to control conduct beyond the boundaries of the State.").

This argument necessarily fails because the express terms of the Anti-Spoofing Act indicate that it does not apply to "[a] caller who, based on the telephone number called, reasonably believes the recipient of the call is not physically located within the state." N.D. Cent. Code § 51-28-08.1(2)(f). Stated another way, to whatever extent a spoofer cannot reasonably determine she is placing a call to a recipient that is physically within the state, the Anti-Spoofing Act simply does not regulate. The Act is neither under-

inclusive or over-inclusive in this respect: it regulates only those calls where it can reasonably be determined the call recipient is physically within North Dakota, and does not regulate those calls where a spoofer reasonably believes the call recipient is not physically within the state.

SpoofCard's contention that it is ***impossible*** to accurately determine the physical location of some call recipients is belied by its own pleadings. SpoofCard admits it has the ability to maintain a "do not spoof" list. See Compl. at ¶ 21, Dist. Ct. Doc. ID #1. SpoofCard admits it can check a "called number to ensure it does not appear on the SpoofCard Do Not Call list." Id. SpoofCard admits it can prevent its customers from making calls to numbers on the list, "[f]or example, 911 centers and certain numbers for law enforcement agencies and financial service companies." Id.

If SpoofCard can place these numbers on a Do Not Call list, it admittedly has the ability to place other numbers on that list that can reasonably be determined are numbers of recipients who are physically located within the state. As the State noted in its previous briefing, SpoofCard can reasonably determine what landline numbers, publicly published either in North Dakota phonebooks or online, are associated with an address physically located in North Dakota. Upon performing its due diligence and research to determine these North Dakota landline numbers, SpoofCard could then place all those numbers on its existing Do Not Call list.

Also, if SpoofCard or its customers call any cell numbers, and the call recipient answers and explains that he or she is physically in North Dakota (whether that number lists a 701 area code or not), SpoofCard would then be placed on reasonable notice that the cell number is in North Dakota. SpoofCard could then place those particular numbers on its Do Not Call list. Further, SpoofCard could also be placed on reasonable notice, in other ways,[2] that a particular phone number is located within the state. Upon being placed

[2] Contrary to SpoofCard's claim that it is "impossible" to determine the physical location of a call recipient who has a cell phone, the technology and means to determine the

on such notice, because of SpoofCard's subsequent reasonable belief that a call recipient is physically within North Dakota, SpoofCard could place those numbers on its Do Not Call list. For example, SpoofCard (and by extension its customers) should be reasonably certain that the number of the Director of the North Dakota Department of Health is physically within North Dakota, or the Bank of North Dakota, or a myriad of other numbers associated with North Dakota state agencies. By limiting its regulatory reach to spoofed calls where there is a reasonable belief that the recipient of the call is physically within the state, the Anti-Spoofing Act does not (indeed, cannot) have the practical effect of regulating conduct that takes place wholly outside the State's borders.

Moreover, the added burdens that SpoofCard might face in complying with the Anti-Spoofing Act's obligation to reasonably determine whether a call recipient is physically within North Dakota do not establish a Commerce Clause violation. See, e.g., Hampton Feedlot, Inc. v. Nixon, 249 F.3d 814, 821 (8th Cir. 2001) ("Economic hardship experienced by [commercial entities] does not rise to the level of a dormant Commerce Clause violation."); Ferguson v. Friendfinders, Inc., 94 Cal. App. 4th 1255, 1265 (Cal. Ct. App. 2002) (rejecting a Healy-based challenge to a statute that regulated deceptive and misleading commercial email sent unsolicited to California residents, brought on the grounds that it was impossible to determine the geographic residence of a recipient, stating the fact that "respondents consider [the statute's] requirements inconvenient and even impractical does not mean that statute violates the commerce clause. Further, if respondents choose to comply with [the statute] all the time (so they can avoid having to

---

physical location of a call recipient through the triangulation of cell phone towers clearly exists. See Richard Miletic, Determining RF Coverage in Criminal Cases, The Gavel, Spring 2019, at 20-24 (found at https://view.joomag.com/spring-2019-gavel-spring-gavel-2019/0644004001557330417?short) (last visited May 7, 2020) (explaining how cell towers can be used in criminal cases to determine the location of a mobile phone at the time of a crime). What SpoofCard means by "impossible" is really just commercial impracticality. But that is not the standard for determining whether North Dakota's law, meant only to regulate calls placed to a location within North Dakota, violates the Commerce Clause.

determine whether they are corresponding with California residents via equipment located in California), that is their business decision. Such a business decision simply does not establish that [the statute] controls conduct occurring wholly outside California.").

SpoofCard's reliance on a Florida district court's decision in TelTech Systems, Inc. v. McCollum, No. 08-61644-CIV-Martinez-Brown, 2009 WL 10626585 (S.D. Fla. July 16, 2009), is misplaced. The Florida law at issue in McCollum did not have a provision excepting from its application calls where the spoofer could not reasonably determine that the recipient of the call was physically within the state. See McCollum, 2009 WL 10626585 at *1-2 (setting forth the provisions of Florida's Anti-Spoofing Act). More significantly, the Court there based its decision on the fact that the defendants did not dispute "that it is impossible for Plaintiffs to know whether the recipient of their Caller ID spoofing is in Florida." Id. at *8. Here, in contrast, SpoofCard admits it has the ability to place calls on a Do Not Call list. This undisputed fact, coupled with the undisputed fact that that there are publicly available phonebooks that link some numbers to physical addresses located in North Dakota, distinguish this case from McCollum. SpoofCard and its customers clearly have the ability to refrain from placing calls to recipients reasonably believed to be in North Dakota. Despite its claims of "impossibility," SpoofCard cannot seriously contest the fact that ***at least some numbers*** can reasonably be linked to physical locations in North Dakota. SpoofCard therefore cannot satisfy the heavy burden of showing the Anti-Spoofing Act violates the Commerce Clause "in all of its applications" and that there is "no set of circumstances . . . under which the Act would be valid." Wash. State Grange v. Wash. State Republican Party, 552 U.S. 442, 449 (2008) (internal quotation marks and citation omitted).

In addition to its Commerce Clause challenge under Healy's extraterritoriality doctrine, SpoofCard also purports to challenge the Anti-Spoofing Act under more traditional dormant Commerce Clause jurisprudence by claiming the Act unduly burdens interstate commerce. See Dist. Ct. Doc. ID #18 at 19-22.

SpoofCard, however, admits the Anti-Spoofing Act regulates even-handedly, that is, there is no discrimination between the regulation of intrastate and interstate commerce. See Dist. Ct. Doc. ID #18, at 20. This concession, coupled with SpoofCard's failure to identify an in-state competitor in the same market, are fatal to SpoofCard's challenge. See Gen. Motors Corp. v. Tracy, 519 U.S. 278, 298 (1997) ("[A]ny notion of discrimination assumes a comparison of substantially similar [in-state and out-of-state] entities"); see also Freedom Holdings Inc. v. Spitzer, 357 F.3d 205, 219 (2d Cir. 2004) (applying Or. Waste Sys. Inc. v. Dep't of Envtl. Quality, 511 U.S. 93 (1994), and holding that "[t]o be prohibited, a [state action] still must favor an in-state commercial interest over a corresponding out-of-state commercial interest"); Town of Southhold v. Town of E. Hampton, 477 F.3d 38, 49 (2d Cir. 2007) (applying Tracy and holding that without an apples-to-apples comparison between "local business vis-à-vis out-of-state competitors" there is no constitutional violation because "laws that draw distinctions between entities that are not competitors do not 'discriminate' for purposes of the dormant Commerce Clause"); Mason & Dixon Lines, Inc. v. Steudle, 761 F. Supp. 2d 611, 626–27 (E.D. Mich. 2011), aff'd, 683 F.3d 289 (6th Cir. 2012) (rejecting the claim that a bridge closure violated the dormant Commerce Clause where there was "no allegation that the defendants' actions discriminate in favor of a *private* [in-state] enterprise" and where the bridge closure "affect[ed] all motorists the same, regardless of state citizenship, and there is no allegation of economic protectionism to support a dormant Commerce Clause challenge").

Tracy instructs that a challenge to state action under the dormant Commerce Clause must include a preliminary showing that the challenged state action impacts competition within a particular common market. 519 U.S. at 298 n.12, 300. In Alliance of Auto. Mfrs., Inc. v. Currey, 984 F. Supp. 2d 32 (D. Conn. 2013), aff'd, 610 F. App'x 10 (2d Cir. 2015), the Court held that a challenge to a statute regulating entities who are not competitors in the same market necessarily "fails to plausibly state a claim of clear

discrimination or, in the alternative, of undue burden on interstate commerce under Pike[3] balancing." Id. at 58. In other words, the threshold failure to identify an in-state competitor in the same market necessarily fails to show an undue burden under Pike's balancing test.

Even assuming SpoofCard's failure to identify an in-state competitor in the same market does not doom its claim and negate the Court's need to conduct an analysis under Pike, any indirect burden the Anti-Spoofing Act may impose on commerce is not clearly excessive in relation to its putative local benefits.

Spoofed calls inundate North Dakota residents with solicitations they do not desire and that are hard to distinguish from useful calls they wish to receive and answer. The Act strengthens the ability of North Dakota to deter fraudulent and harmful spoofing by assisting North Dakota consumers in filtering unwanted calls. Consumer protection against fraud is a traditional state police power. In re Aurora Dairy Corp. Organic Milk Mktg. & Sales Practices Litig., 621 F.3d 781, 794 (8th Cir. 2010). North Dakota wants to protect its citizens and businesses from the costs associated with receiving fraudulent and harmful spoof calls. The Act also economically benefits and protects these citizens and businesses of North Dakota, while only "tangentially" burdening interstate commerce. See, e.g., People by Vacco v. Lipsitz, 663 N.Y.S.2d 468, 475 (N.Y. Sup. Ct. 1997) (concluding a New York consumer protection law that targeted the use, misuse, and abuse of e-mail did not unduly burden commerce under Pike).

Potential nefarious uses for spoofing are obvious and virtually limitless. Examples include callers who may be: falsely pretending to be affiliated with certain organizations; lying to employers about their workplace status; misappropriating identities; or perpetuating identity theft scams. The high value to criminals of various spoofing

[3] Pike v. Bruce Church, Inc., 397 U.S. 137 (1970).

techniques, as a tool for fraudulent activities, is well documented.[4] On January 7, 2013, for example, the Internet Crime Complaint Center issued a scam alert for various denial-of-service attacks by which fraudsters were using spoofed Caller ID to impersonate police in an attempt to collect bogus payday loans, and then placing repeated harassing calls to police with the victim's number displayed.[5] Other scams involved impersonating utility companies to threaten businesses or householders with disconnection,[6] as a means to extort money,[7] impersonating immigration officials[8] or impersonating medical insurers to obtain personal data for use in theft of identity.[9] Bogus caller ID has also been used in grandparent scams, which unconscionably target the elderly by impersonating family members and requesting wire transfers of money.[10]

SpoofCard argues that "making it a crime to waste the time of a party that answers the phone" is the only discernable benefit from the Act. Dist. Ct. Doc. ID #18 at 21. The numerous nefarious uses of spoofing to perpetrate fraud, the hundreds of hours of law enforcement time spent investigating that fraud, and the actual losses that victims suffer show this to be false. On the other hand, SpoofCard argues the burdens imposed on it

---

[4] For example, in 2009, the U.S. Senate Committee on Commerce, Science, and Transportation, issued a report identifying numerous potential harmful uses of spoofing. The Committee chronicled several publicized instances where spoofing has been used in connection with criminal conduct including jury duty scams, fake emergency calls, and identity theft. See Truth in Caller ID Act of 2009, Report of the Committee on Commerce, Science, and Transportation on S.30, Report 111-96 at 1-2 (Nov. 2, 2009).

[5] Internet Crime Complaint Center's (IC3) Scam Alerts (January 7, 2013), https://www.ic3.gov/media/2013/130107.aspx (last visited May 7, 2020).

[6] Gary Gerew, FTC asked to probe fraudulent calls to restaurants, Albuquerque Business First (Oct. 1, 2013, 9:35 AM) https://www.bizjournals.com/albuquerque/blog/morning-edition/2013/10/ftc-asked-to-probe-fraudulent-calls.html (last visited May 7, 2020).

[7] Nick Sloan, BPU warns customers of phone-scam, Kansas City Kansan (October 14, 2013), http://www.kckansan.com/2013/10/bpu-warns-customers-of-phone-scam.html (last visited May 7, 2020).

[8] Beware: widespread immigration-related fraud schemes currently on the rise, Lexology, https://www.lexology.com/library/detail.aspx?g=c006d7c3-8e53-4f77-b90e-6bfd6d8e4538 (last visited May 7, 2020).

[9] Jack Smith IV, Scammers busy under guise of Obamacare", CBS News (Oct. 9, 2013, 2:51 PM), https://www.cbsnews.com/news/scammers-busy-under-guise-of-obamacare/ (last visited May. 9, 2020).

[10] Watch Out for 'Grandparent' Scams, Federal Communications Commission, https://www.fcc.gov/watch-out-grandparent-scams (last visited May7, 2020).

are substantial, citing the financial costs of compliance. Id. But to continue the legitimate deceptive spoofing of its customers, SpoofCard need only place those phone numbers it reasonably believes are located in North Dakota on its already established Do Not Call list. The Anti-Spoofing Act does not prevent solicitors from calling any individual in North Dakota; it only prevents them from doing so using "misleading or inaccurate caller identification information with the intent to defraud or cause harm; or [using] or display[ing] a telephone number the caller does not own or has received consent to use from the owner of the telephone number." N.D. Cent. Code § 51-28-08.1(1). The State's regulatory interest in preventing fraud and property theft/misuse clearly outweigh any indirect burden this neutral regulatory law has on commerce.

The State, through the lawful exercise of its sovereign police powers in promulgating the Act, did not run afoul of the Commerce Clause. In determining whether a state law imposes a clear and excessive burden on interstate commerce, a court must consider that the Constitution "never intended to cut the States off from legislating on all subjects relating to the health, life, and safety of their citizens," even if the law may indirectly affect interstate commerce. Huron Portland Cement Co. v. City of Detroit, Mich., 362 U.S. 440, 443 (1960). Rather, "[s]tate regulation, based on the police power, which does not discriminate against interstate commerce . . . may constitutionally stand." Id. at 448.

In light of North Dakota's retained police powers, the Anti-Spoofing Act's purported enhancement to the overall economic welfare justifies any insubstantial extraterritorial effects of the Act that are alleged by SpoofCard. The Act significantly enhances the overall economic welfare of North Dakota. Not only is the Act reasonable, but the Legislature is owed extensive deference in its decision to promulgate further regulatory oversight over deceptive telecommunications occurring within its borders. See, e.g., United States Tr. Co. of N.Y. v. New Jersey, 431 U.S. 1, 22-23 (1977) (noting that courts, when reviewing state economic legislation, "properly defer to legislative judgment as to

the necessity" of the measures at issue).

CONCLUSION

For the reasons stated above, the State respectfully requests that SpoofCard's motion for partial summary judgment be denied. In addition, the State requests that its cross-motion for summary judgment on the issues of preemption and the Commerce Clause be granted.

Dated this 8th day of May, 2020.

State of North Dakota
Wayne Stenehjem
Attorney General

By: /s/ James E. Nicolai
James E. Nicolai
Deputy Solicitor General
State Bar ID No. 04789
Office of Attorney General
500 North 9th Street
Bismarck, ND 58501-4509
Telephone (701) 328-3640
Facsimile (701) 328-4300
Email jnicolai@nd.gov

Attorneys for Defendant.